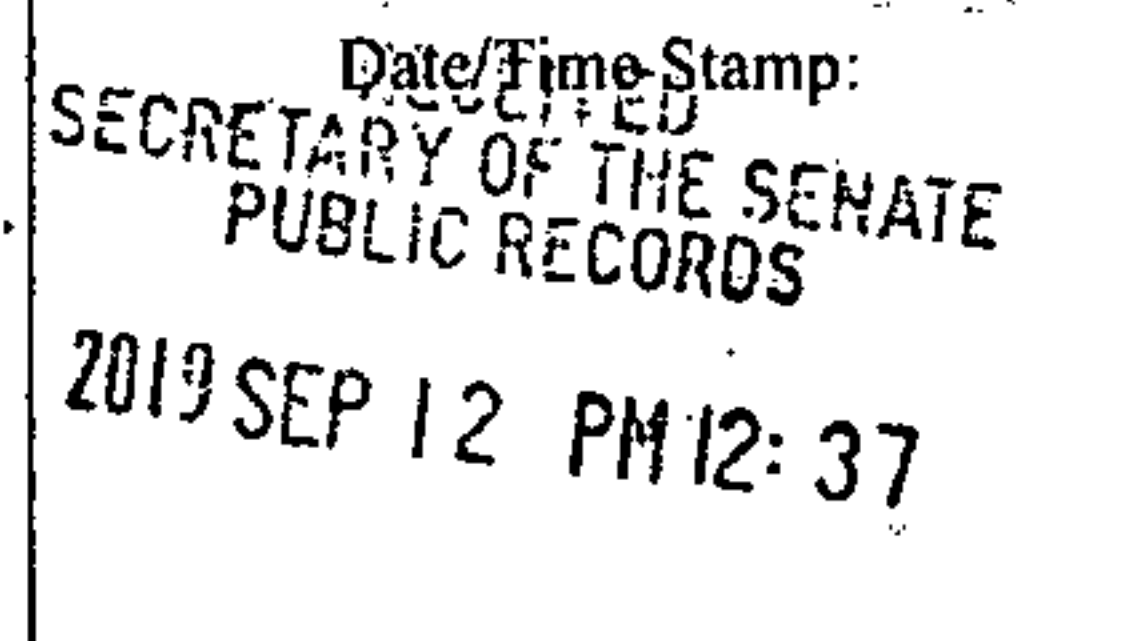# Employee Post-Travel Disclosure of Travel Expenses

Post-Travel Filing Instructions: Complete this form within **30 days** of returning from travel. Submit all forms to the **Office of Public Records in 232 Hart Building.**

In compliance with Rule 35.2(a) and (c), I make the following disclosures with respect to travel expenses that have been or will be reimbursed/paid for me. I also certify that I have attached:

☒ The **original** *Employee Pre-Travel Authorization* (Form RE-1), **AND**

☒ A **copy** of the *Private Sponsor Travel Certification Form* with all attachments (itinerary, invitee list, etc.)

Private Sponsor(s) (list all): **Stanford University**

Travel date(s): **26-29 August 2019**

Name of accompanying family member (if any): **NOT APPLICABLE**

Relationship to Traveler: ☐ Spouse   ☐ Child

IF THE COST OF LODGING **DID NOT INCREASE** DUE TO THE ACCOMPANYING SPOUSE OR DEPENDENT CHILD, ONLY INCLUDE LODGING COSTS IN EMPLOYEE EXPENSES. (Attach additional pages if necessary.)

Expenses for Employee:

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses (Amount & Description)
☐ Good Faith Estimate ☒ Actual Amount	$599.45 Airfare $60 Grd Trans	$600 ($200/night x 3 nights)	$231	None

Expenses for Accompanying Spouse or Dependent Child (if applicable):

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses (Amount & Description)
☐ Good Faith Estimate ☐ Actual Amount	N/A	N/A	N/A	N/A

Provide a description of all meetings and events attended. *See* Senate Rule 35.2(c)(6). (Attach additional pages if necessary.): Attended the Stanford University Congressional AI/Cyber Bootcamp from 26-29 August 2019 at Stanford University, California

Full itinerary and other details are attached.

10 Sept 19
(Date)

JOHN S. RIORDAN
(Printed name of traveler)

(Signature of traveler)

TO BE COMPLETED BY SUPERVISING MEMBER/OFFICER:

I have made a determination that the expenses set out above in connections with travel described in the *Employee Pre-Travel Authorization* form, are necessary transportation, lodging, and related expenses as defined in Rule 35.

9/10/2019
(Date)

(Signature of Supervising Senator/Officer)

(Revised 1/3/11)   Form RE-2

EMPLOYEE PRE-TRAVEL AUTHORIZATION

Pre-Travel Filing Instructions: Complete and submit this form at least 30 days prior to the travel departure date to the **Select Committee on Ethics in SH-220.** Incomplete and late travel submissions will **not** be considered or approved. This form **must** be typed and is available as a fillable PDF on the Committee's website at ethics.senate.gov. Retain a copy of your entire pre-travel submission for your required post-travel disclosure.

Name of Traveler: _____ John Stephen Riordan _____

Employing Office/Committee: _____ Senate Armed Services Committee _____

Private Sponsor(s) (list all): Stanford University _____

Travel date(s): 26-29 August 2019 _____
       *Note: If you plan to extend the trip for any reason you **must** notify the Committee.*

Destination(s): Stanford University, Stanford, California _____

Explain how this trip is specifically connected to the traveler's official or representational duties:

> This course will contribute to my knowledge on AI and Cyber in supporting Members of Congress in their deliberations on the National Defense Authorization Act (NDAA.) As the Strategic Forces Subcommittee Staff lead, I interact with experts daily that provide information that can affect support for members of the Armed forces, as well as impact the proper execution of our national Defense Strategy. including Space, Missile Defense and Nuclear matters. This course can help inform my decisions In supporting and/or modifying programs to support our Armed forces.

Name of accompanying family member (if any): None _____

Relationship to Employee: ☐ Spouse   ☐ Child

I certify that the information contained in this form is true, complete and correct to the best of my knowledge:

____12 August 2019____   _____
     (Date)   *(Signature of Employee)*

TO BE COMPLETED BY SUPERVISING SENATOR/OFFICER (President of the Senate, Secretary of the Senate, Sergeant at Arms, Secretary for the Majority, Secretary for the Minority, and Chaplain):

I, _____ Senator Jim Inhofe (R-OK) _____ hereby authorize _____ John Stephen Riordan _____
     (Print Senator's/Officer's Name)   *(Print Traveler's Name)*

an employee under my direct supervision, to accept payment or reimbursement for necessary transportation, lodging, and related expenses for travel to the event described above. I have determined that this travel is in connection with his or her duties as a Senate employee or an officeholder, and will not create the appearance that he or she is using public office for private gain.

I have also determined that the attendance of the employee's spouse or child is appropriate to assist in the representation of the Senate. (*signify "yes" by checking box*) ☐

____13 AUG 2019____   _____
     (Date)   *(Signature of Supervising Senator/Officer)*

                               (Form RE-1)

PRIVATE SPONSOR TRAVEL CERTIFICATION FORM

This form must be completed by any private entity offering to provide travel or reimbursement for travel to Senate Members, officers, or employees (Senate Rule 35, clause 2). Each sponsor of a fact-finding trip must sign the completed form. The trip sponsor(s) must provide a copy of the completed form to each invited Senate traveler, who will then forward it to the Ethics Committee with any other required materials. The trip sponsor(s) should **NOT** submit the form directly to the Ethics Committee. Please consult the accompanying instructions for more detailed definitions and other key information.

The Senate Member, officer, or employee **MUST** also provide a copy of this form, along with the appropriate travel authorization and reimbursement form, to the Office of Public Records (OPR), Room 232 of the Hart Building, within thirty (30) days after the travel is completed.

1. Sponsor(s) of the trip (please list all sponsors): Stanford University

2. Description of the trip: An intensive program for Congressional staff which consists of three days of seminars, simulations, and keynote presentations.

3. Dates of travel: August 26-29, 2019

4. Place of travel: Stanford University, Stanford, CA

5. Name and title of Senate invitees: See attached list.

6. I *certify* that the trip fits one of the following categories:

   ☐ (A) The sponsor(s) are not registered lobbyists or agents of a foreign principal **and** do not retain or employ registered lobbyists or agents of a foreign principal **and** no lobbyist or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

   – OR –

   ☒ (B) The sponsor or sponsors are not registered lobbyists or agents of a foreign principal, but retain or employ one or more registered lobbyists or agents of a foreign principal and the trip meets the requirements of Senate Rule 35.2(a)(2)(A)(i) or (ii) *(see question 9)*.

7. ☒ I *certify* that the trip will not be financed in any part by a registered lobbyist or agent of a foreign principal.

   – AND –

   ☒ I *certify* that the sponsor or sponsors will not accept funds or in-kind contributions earmarked directly or indirectly for the purpose of financing this specific trip from a registered lobbyist or agent of a foreign principal or from a private entity that retains or employs one or more registered lobbyists or agents of a foreign principal.

8. I *certify* that:

   ☒ The trip will not in any part be planned, organized, requested, or arranged by a registered lobbyist or agent of a foreign principal except for *de minimis* lobbyist involvement.

   – AND –

   ☒ The traveler will not be accompanied on the trip by a registered lobbyist or agent of a foreign principal except as provided for by Committee regulations relating to lobbyist accompaniment *(see question 9)*.

PSTC FORM

9. **USE ONLY IF YOU CHECKED QUESTION 6(B)**
   I *certify* that if the sponsor or sponsors retain or employ one or more registered lobbyists or agents of a foreign principal, one of the following scenarios applies:

   ☐ (A) The trip is for attendance or participation in a one-day event (exclusive of travel time and **one** overnight stay) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip.
   $$- \text{OR} -$$

   ☐ (B) The trip is for attendance or participation in a one-day event (exclusive of travel time and **two** overnight stays) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip (*see questions 6 and 10*).
   $$- \text{OR} -$$

   ☒ (C) The trip is being sponsored only by an organization or organizations designated under § 501(c)(3) of the Internal Revenue Code of 1986 and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

10. **USE ONLY IF YOU CHECKED QUESTION 9(B)**
    If the trip includes two overnight stays, please explain why the second night is practically required for Senate invitees to participate in the travel:

    _____

    _____

    _____

11. ☒ An itinerary for the trip is attached to this form. I *certify* that the attached itinerary is a detailed (hour-by-hour), complete, and final itinerary for the trip.

12. Briefly describe the role of each sponsor in organizing and conducting the trip:

    Stanford University solely planned all aspects of the trip including topics discussed, travel/accommodation

    logistics, and required paperwork. Stanford staff will also be responsible for traveling with Congressional

    staff and managing logistics for the duration of the trip.

13. Briefly describe the stated mission of each sponsor and how the purpose of the trip relates to that mission:

    Stanford University is a 501(C)3 institution of higher education that seeks to promote the public welfare by

    excercising an influence in behalf of humanity and civilization, through teaching and rigorous scholarship.

    _____

14. Briefly describe each sponsor's prior history of sponsoring congressional trips:

    This is the fourth Cyber Boot Camp for Congressional staff organized by Stanford. The most recent one

    was August 2017 and had a similar format to this trip.

    _____

15. Briefly describe the educational activities performed by each sponsor (other than sponsoring congressional trips):

Stanford University regularly sponsors policy panels and roundtables for think tanks scholars, journalists,

Congressional staff, Executive branch officials, academics and members of the public. Additionally

Stanford educates numerous undergrad and graduate students within the university.

16. Total Expenses for Each Participant:

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses
☒ Good Faith estimate ☐ Actual Amounts	$599.45 Round trip airfare $60 ground transportation	$600 ($200/night)	$231	

17. State whether a) the trip involves an event that is arranged or organized *without regard* to congressional participation **or** b) the trip involves an event that is arranged or organized *specifically with regard* to congressional participation:

The trip involves an event that is arranged/organized specifically with regard to Congressional staff

participation.

18. Reason for selecting the location of the event or trip

In order to have a significant number of California-based faculty participate in the event, we are hosting

it at the Stanford University campus.

19. Name and location of hotel or other lodging facility:

Schwab Residential Center, 680 Serra Street, Stanford CA 94305

20. Reason(s) for selecting hotel or other lodging facility:

The Schwab Residential Center is owned and operated by Stanford University. It is in close proximity to

the events that compromise the program, and falls into the per diem guidelines.

21. Describe how the daily expenses for lodging, meals, and other expenses provided to trip participants compares to the maximum per diem rates for official Federal Government travel:

Lodging expenses are less than the federal per diem for Palo Alto, CA. Meal expenses are less than the

federal per diem for Palo Alto, CA.

22. Describe the type and class of transportation being provided. Indicate whether coach, business-class or first class transportation will be provided. If first-class fare is being provided, please explain why first-class travel is necessary:

Stanford University will provide economy class round trip airfare between Washington, DC and

San Francisco, CA, and round trip ground transportation between Stanford University and SFO

23. ☒ I represent that the travel expenses that will be paid for or reimbursed to Senate invitees do not include expenditures for recreational activities, alcohol, or entertainment (other than entertainment provided to all attendees as an integral part of the event, as permissible under Senate Rule 35).

24. List any entertainment that will be provided to, paid for, or reimbursed to Senate invitees and explain why the entertainment is an integral part of the event:

None.

25. I hereby *certify* that the information contained herein is true, complete and correct. (For trips involving more than one sponsor, you *must* include a completed signature page for each additional sponsor):

Signature of Travel Sponsor: _____

Name and Title: Russell Wald, Senior Manager, External Affairs

Name of Organization: Stanford University

Address: 434 Galvez Mall, Stanford, CA 94305

Telephone Number: 202.760.3200

Fax Number: 202.760.3191

E-mail Address: rwald@stanford.edu

PRIVATE SPONSOR TRAVEL CERTIFICATION FORM
SIGNATURE PAGE FOR ADDITIONAL SPONSOR
(to be completed by each additional sponsor)

I hereby *certify* that the information contained on pages 1-4 of the certification form and any accompanying addenda, all submitted in connection with the August 26-29, 2019 trip

Dates of Travel (Month Day, Year)

to Stanford University, Stanford, CA is true, complete, and correct.

Place of Travel

Signature of Travel Sponsor: _____

Name and Title: Russell Wald, Senior Manager, External Affairs

Name of Organization: Stanford University

Address: 434 Galvez Mall, Stanford, CA 94305

Telephone Number: 202-760-3200

Fax Number: 202-760-3191

E-mail Address: rwald@stanford.edu

United States Senate

SELECT COMMITTEE ON ETHICS

August 21, 2019

John Stephen Riordan
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Riordan:

This responds to your recent correspondence concerning an invitation you received to travel to the *Stanford Cyber and Artificial Intelligence Boot Camp* in Stanford, California, on August 26–29, 2019, sponsored by Stanford University (Stanford). Stanford certified to the Select Committee on Ethics (the Committee) that it will pay the *necessary expenses*[1] related to the travel and that it is neither a lobbyist, nor lobbying firm, nor agent of a foreign principal, and it is not otherwise acting as a representative or agent of a foreign government. However, Stanford has certified that it is an organization designated under § 501(c)(3) of the Internal Revenue Code[2] that retains or employs a registered lobbyist and that no registered lobbyist or agent of a foreign principal will accompany you at *any point throughout your trip*.[3]

Based on information and materials available to the Committee, and assuming the **actual** travel and travel-related expenses conform to the information and materials you provided, it appears that the proposed payment or reimbursement of necessary expenses for this trip **may be accepted** under relevant Senate Rules and the Committee's *Regulations and Guidelines for Privately-Sponsored Travel*, so long as at the time of the payment or reimbursement, Stanford is neither a registered lobbyist nor lobbying firm under the Lobbying Disclosure Act of 1995, nor an agent of a foreign principal under the Foreign Agents Registration Act (and is not otherwise acting as a representative or agent of a foreign government), and provided the travel and all required documents are disclosed to the Secretary of the Senate in accordance with the provisions of Senate Rules 34 and 35.

Under Senate Rule 35, Senate staff must receive advance authorization signed by the Member or officer under whose direct supervision the individual works in order to accept payment or reimbursement for necessary expenses related to fact-finding travel. Further, such authorization and expenses must be disclosed to the Secretary of the Senate by filing the completed *Employee Pre-Travel Authorization* and the *Employee Post-Travel Disclosure of Travel Expenses* (Form RE-1 and Form RE-2), along with a copy of the *Private Sponsor Travel*

---

[1] The term "necessary expenses" has a specific definition. *See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms* at 8.

[2] 26 U.S.C. § 501(c)(3).

[3] The term "any point throughout your trip" has a specific definition. *See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms* at 2.

Certification Form, and all relevant attachments (e.g., the private sponsor's invitation and itinerary) **within 30 days of the conclusion of Privately-Sponsored Travel.**

Finally, Senate Rule 34 requires a reporting individual,[4] on his or her Financial Disclosure Report, to make an annual disclosure of the receipt of payments or reimbursements under Senate Rule 35 from a private sponsor for officially-related travel expenses where, in the aggregate, travel expenses exceed $390 from that sponsor during a calendar year. However, if a Member, officer, or employee properly reports the receipt of necessary expenses for such travel to the Secretary of the Senate within 30 days of the travel, as discussed above, the travel expenses need not be disclosed a second time on their Financial Disclosure Report.

I hope you find this information helpful. If you have any additional questions, please do not hesitate to contact the Committee.

Sincerely,

Deborah Sue Mayer
Chief Counsel and Staff Director

Enclosure: Travel Checklist

---

[4] A reporting individual is someone whose salary equals or exceeds 120% of the basic rate of pay for GS-15 ($127,914 for CY 2019) or is a political fund designee and is required to file Financial Disclosure Reports.

CYBER AND ARTIFICIAL INTELLIGENCE BOOT CAMP
AUGUST 26-29, 2019

Institute for
International Studies

HOOVER
INSTITUTION

July 18, 2019

Dear Mr. Riordan,

We are pleased to inform you that you have been selected to participate in the Stanford Cyber and Artificial Intelligence Boot Camp at Stanford University in Palo Alto, CA, on August 26th – 29th. This intensive 3-day program includes seminars, simulations, a keynote dinner event with industry stakeholders, and a field trip.

These sessions will challenge you to learn from and debate key philosophical and policy issues with some of the nation's leading thinkers and practitioners. As a participant you will receive round-trip airfare and ground transportation to Stanford University from Washington, DC, housing on Stanford's campus, and those meals that are part of the program.

To proceed, please confirm your agreement to attend by completing <u>this form</u> by the close of business on Monday, July 22nd. Due to ethics rules, to maintain your spot, it is imperative that you submit the proper paperwork. Please complete the paperwork provided and items listed below **to your ethics committee for review by Wednesday, July 24th**. Your submission packet must include:

- Traveler Form (attached for you to fill out)
- Private Sponsor Certification Form (completed for you and attached)
- Syllabus
- Senate Boot Camp Offers
- Copy of this invitation letter

If you have any questions, do not hesitate to contact me (<u>rwald@stanford.edu</u>). Thank you in advance for your prompt response so we can ensure your seat in the boot camp. We look forward to and expect an excellent program.

Sincerely,

Russell C. Wald
Senior Manager, External Affairs
Hoover Institution, Stanford University

United States Senate

SELECT COMMITTEE ON ETHICS

<u>Employee Privately-Sponsored Travel Checklist</u>

Employees must submit their completed Pre-Travel Authorization Package to the Select Committee on Ethics (the Committee) **at least 30 days** prior to the travel departure date. Incomplete Pre-Travel Authorization Packages and Packages submitted later than 30 days prior to the travel departure date will not be considered or approved. All of the forms and materials listed below are available as fillable PDFs on the Committee's website at <u>http://www.ethics.senate.gov</u>.

<u>Pre-Travel Authorization</u>

<u>Prior to Submitting a Pre-Travel Authorization Package to the Committee</u>

- ❑ Review Senate Rules and the Committee's Privately-Sponsored Travel Guidelines on the Committee's website.
  - ❑ Ensure your supervising Senator or Officer (President of the Senate, Secretary of the Senate, Sergeant at Arms, Secretary for the Majority, Secretary for the Minority, and Chaplain) has determined the expenses for the trip are necessary and reasonable.
  - ❑ Ensure your supervising Senator or Officer has certified the proposed travel is connected to your official duties and will not create any appearance of a public office being used for private gain.

<u>At Least 30 Days Prior to Travel: Submit Completed Pre-Travel Authorization Package</u>
File with the Select Committee on Ethics in SH-220

- ❑ Complete Employee Pre-Travel Authorization Form (Form RE-1)
  - ❑ Ensure this form is typed and that all of the fields are completed.
  - ❑ Ensure your supervising Senator or Officer has signed this form.
  - ❑ Personally sign this form.
- ❑ Ensure Pre-Travel Authorization Package is complete. A complete Package includes:
  - ❑ Form RE-1
  - ❑ Private sponsor invitation (the formal invitation, letter or e-mail you received from the private sponsor).
  - ❑ Completed and signed Private Sponsor Travel Certification Form (4 page form that includes detailed information about the trip).
  - ❑ All attachments to the Private Sponsor Travel Certification Form
    - ❑ Complete and final itinerary
    - ❑ List of Senate invitees
    - ❑ Any other necessary attachments
- ❑ Retain a copy of your complete Pre-Travel Authorization Package for inclusion in your required post-travel disclosure.

<u>Prior to Traveling: Receive a Letter of Approval from the Committee</u>

❑ Obtain a letter from the Committee. You may only accept the trip after receiving a letter from the Committee specifically authorizing your participation in the privately-sponsored travel.

Post-Travel Disclosure

<u>Within 30 Days of Conclusion of Privately-Sponsored Travel: Submit Completed Post-Travel Disclosure Package</u>
File with the Office of Public Records in SH-232

☒ Ensure submission of Post-Travel Disclosure Package is timely.
  ☒ Post-Travel Disclosure Packages must be submitted to the Office of Public Records within 30 days of completion of Privately-Sponsored Travel. Trip extensions for any purpose do not extend this deadline.
☒ Complete Employee Post-Travel Disclosure of Expenses Form (Form RE-2)
  ☒ Ensure this form is typed and that all of the fields are completed.
  ☒ Ensure your supervising Senator or Officer has signed the form after determining the actual trip expenses were necessary under Senate Rules and the Committee's Privately-Sponsored Travel Guidelines.
  ☒ Personally sign this form.

ALL
INCLUDED

☒ Ensure Post-Travel Disclosure Package is complete. A complete Package includes:
  ☒ Form RE-1
  ☒ Form RE-2
  ☒ Private sponsor invitation (the formal invitation, letter or e-mail you received from the private sponsor).
  ✓ ☒ Completed and signed Private Sponsor Travel Certification Form (<u>verify</u> with the private sponsor that you have the <u>correct and final version</u> of the form).
  ☒ All attachments to the Private Sponsor Travel Certification Form
    ☒ Complete and final itinerary
    ☒ List of Senate invitees
    ☒ Any other necessary attachments

Please contact the Committee if you have any questions.

Phone: (202)-224-2981
Fax: (202)-224-7416

JOHN S. RIORDAN
SASC PSM
X4-6371

UNITED | TSA Pre✓

RIORDAN/JOHNSTEPHEN

UA- ''757

San Francisco to Washington-Dulles

UA 516	GATE	BOARDING BEGINS		SEAT
	SFO-IAD 74	8:50 AM		37A

THU 29 AUG 20   Gate May Change

Boarding Ends: 9:15 AM   Window
Flight Departs: 9:30 AM   Economy
Flight Arrives: 5:42 PM

KZM01G

MileagePlus   KZM01G
eTicket No. 1937907501
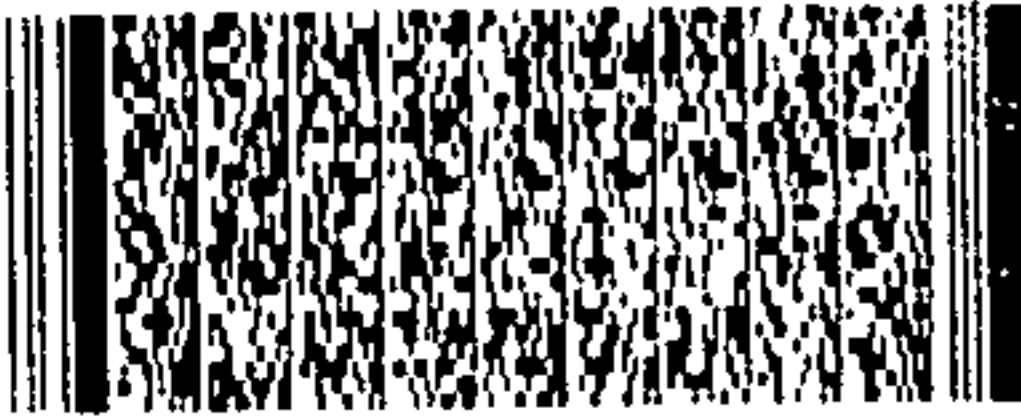
KZM01G   37A   145
UA 516   ESF00071

STAR ALLIANCE MEMBER ✦

BOARDING GROUP **3**

UNITED | TSA Pre✓

RIORDAN/JOHNSTEPHEN

UA- ''757

Washington-Dulles to San Francisco

UA1881	GATE	BOARDING BEGINS		SEAT
	IAD-SFO D23	6:20 AM		31C

MON 26 AUG 2019   Gate May Change

Boarding Ends: 6:45 AM   Aisle
Flight Departs: 7:00 AM   Economy
Flight Arrives: 9:49 AM

Confi   8738379075801

KZM01G

KZM01G   31C   81
UA1881   EIAD0051

A STAR ALLIANCE MEMBER ✦

BOARDING GROUP **4**

CYBER AND ARTIFICIAL INTELLIGENCE BOOT CAMP
AUGUST 26-29, 2019

Freeman Spogli Institute for International Studies | HOOVER INSTITUTION | HAI
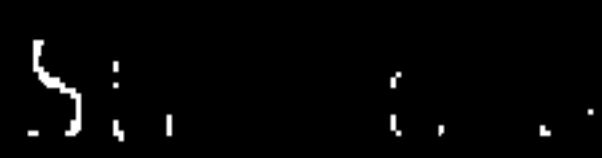
Cyber and Artificial Intelligence Boot Camp Calendar

The Hoover Institution, Annenberg Conference Room 105, Lou Henry Hoover Building
434 Galvez Mall, Stanford, CA 94385

Monday, August 26 Cyber Offense & Defense	Tuesday, August 27 Technical and Nontechnical Approaches	Wednesday, August 28 Industry Voices & the Future of AI
9:50am Group flight arrives at SFO	8:30am-9:00am **Debrief Breakfast** Andrew Grotto, Herb Lin 9:00am-11:00am **Hands On Hack Lab** Alex Stamos	9:00am-9:30am **Debrief Breakfast** Andrew Grotto, Herb Lin 9:30am-10:45am **Industry Perspectives Panel** Raj Shah (chair), Frank Chen, Michelle Finneran Dennedy, Rick Howard, Mark Rosekind
11:30am-12:00pm **Introduction and Program Overview** Andrew Grotto, Herb Lin	11:15am-12:15pm **Cyber Risk, Economics, and Organizational Dimensions of Cyberspace Lunch** Tyler Moore, Greg Falco	11:00am-12:00pm **Fundamentals of AI and Machine Learning** Emma Brunskill, Jeff Clune
12:00pm-12:30pm **Keynote Lunch Address** H.R. McMaster 12:30pm-1:30pm **Thinking Like an Attacker** Greg Conti, Herb Lin	12:30pm-1:30pm **Privacy & Security for Consumers, Customers, and Critical Infrastructure** Robert Chesney, Jennifer King, Ted Gizewski	12:15pm-1:15pm **Keynote Lunch: Artificial Intelligence and Safety** Fei-Fei Li, Mykel Kochenderfer
1:45pm-3:00pm **Current Threat Landscape** Kevin Mandia, Sean Kanuck 3:15pm-4:15pm **Threats to Cybersecurity** Carey Nachenberg, Tom Berson	1:45pm-2:45pm **International Law and Cybersecurity** Tess Bridgeman, Herb Lin 2:45pm-3:45pm **Fundamentals of Defense for Cybersecurity** Irving Lachow, Andrew Grotto	1:30pm-2:30pm **Ethics and Governance for AI** John Villasenor, Patrick Lin 2:40pm-3:50pm **Hoover Tower, Library and Archives Tour (staffers only)**
4:30pm-5:30pm **Offensive Dimensions of Cybersecurity Dinner** Jason Kichen, Herb Lin	4:00pm-5:00pm **Cyber Enabled Information Warfare and Influence Operations** Rosanna Guadagno, Herb Lin	4:15pm-5:30pm **Visit to Center for Automotive Research at Stanford (staffers only)** Stephen Zoepf, Bryan Casey, Marco Pavone
6:00pm-8:30pm **Hospital Ransomware Simulation (staffers only)**	6:30pm-9:00pm **Artificial Intelligence Keynote Reception and Dinner** John Etchemendy, Reid Hoffman, Michael McFaul	6:00pm-8:00pm **Dinner & Participant Reflections (staffers only)** Stanford Golf Course

Thursday, August 29: 9:30am Group flight departs from SFO

◼ Gmail

John Riordan <

Ticket Itinerary and Receipt for Confirmation KZM01G
1 message

United Airlines, Inc. <Receipts@united.com>   Mon, Jul 9 PM
To:

UNITED ▨.

Thank you for choosing United.
A receipt of your purchase is shown below. Please retain this email receipt for your re

Confirmation Number:

KZM01G

Flight 1 of 2 UA1881   C

Mon, Aug 26, 2019	Aug
07:00 AM	**09:49**
Washington, DC, US (IAD)	San Francisco, CA, US (SFO)

Flight 2 of 2 UA516   Class: W

Thu, Aug 29, 2019	Thu, Aug 29, 2019
09:30 AM	**05:42 PM**
San Francisco, CA, US (SFO)	Washington, DC, US (IAD)

Traveler Details

ABBEY/TRISTANCORNELIUS
eTicket number: **0167383455234**   Seats: **IAD-SFO -**
Frequent Flyer: **UA-XXXXX078 Member**   **SFO-IAD -**

ARIAS/KAROLINAMARIE
eTicket number: **0167383455235**   Seats: **IAD-SFO -**
                                        SFO-IAD -

BARRERA/VIRGILIO
eTicket number: **0167383455236**   Seats: **IAD-SFO -**
Frequent Flyer: **UA-XXXXX794 Member**   **SFO-IAD -**

BARTON/JACOBERROL

eTicket number: **0167383455237**

Frequent Flyer: **UA-XXXX673 Premier 1K®**

Seats: **IAD-SFO -**

SFO-IAD -----

BROWN/DEVRON

eTicket number: **0167383455238**

Frequent Flyer: **UA-XXXX902 Member**

Seats: **IAD-SFO -**

SFO-IAD -

CARITHERS/CHARLESANDERSON

eTicket number: **0167383455239**

Frequent Flyer: **UA-XXXX141 Member**

Seats: **IAD-SFO -**

SFO-IAD -----

FULLERTON/LAURAFUNDERBURK

eTicket number: **0167383455240**

Frequent Flyer: **UA-XXXX631 Premier Silver**

Seats: **IAD-SFO -----**

SFO-IAD -

HARRIS/KATHERINECLARK

eTicket number: **0167383455241**

Frequent Flyer: **UA-XXXX377 Premier Silver**

Seats: **IAD-SFO -**

SFO-IAD -

KIM/SUNMIN

eTicket number: **0167383455242**

Frequent Flyer: **UA-XXXX824 Member**

Seats: **IAD-SFO -**

SFO-IAD -

MATT/SVETLANA

eTicket number: **0167383455244**

Frequent Flyer: **UA-XXXX039 Member**

Seats: **IAD-SFO -**

SFO-IAD -

MOXLEY/SARAHWHITING

eTicket number: **0167383455245**

Frequent Flyer: **UA-XXXX076 Member**

Seats: **IAD-SFO -**

SFO-IAD -

OLIDORT/JACOB

eTicket number: **0167383455246**

Seats: **IAD-SFO -----**

SFO-IAD -

PASCOE/CHERILYNELIZABETH

eTicket number: **0167383455247**

Frequent Flyer: **UA-XXXX964 Member**

Seats: **IAD-SFO -**

SFO-IAD -----

PAYNE/WILLIAMROBERT

eTicket number: **0167383455248**

Frequent Flyer: **UA-XXXX311 Member**

Seats: **IAD-SFO -**

SFO-IAD -----

RAMZANALI/ASAD

eTicket number: **0167383455249**

Frequent Flyer: **UA-XXXX533 Member**

Seats: **IAD-SFO -----**

SFO-IAD -

RIORDAN/JOHNSTEPHEN

eTicket number: **0167383790750**

Seats: **IAD-SFO -**

Frequent Flyer: **UA-XXXXX757 Member**   **SFO-IAD** -

SEEDS/MICHAELWILLIAM

eTicket number: **0167383790752**   Seats: **IAD-SFO** -----
                                                                     SFO-IAD -

SIMMS/VERNONLAFRANCIS

eTicket number: **0167383790753**   Seats: **IAD-SFO** -----
                                                                     SFO-IAD -

TROCCHIO/CLINTONALBERT

eTicket number: **0167383790754**   Seats: **IAD-SFO** -----
                                                                     SFO-IAD -----

SULFAB/ELMAMOUNYOUSIF

eTicket number: **0167383790755**   Seats: **IAD-SFO** -----
                                                                     SFO-IAD -----

TAI/KATHERINECHI

eTicket number: **0167383790756**   Seats: **IAD-SFO** -
Frequent Flyer: **UA-XXXXX858 Premier Silver**   **SFO-IAD** -

WHITE/JENNIFERHENDRIXSON

eTicket number: **0167383790757**   Seats: **IAD-SFO** -
Frequent Flyer: **UA-XXXXX250 Premier 1K®**   **SFO-IAD** -

WINKLER/ROBERTPAUL

eTicket number: **0167383790758**   Seats: **IAD-SFO** -
Frequent Flyer: **UA-XXXXX052 Premier Platinum**   **SFO-IAD** -

HAGENSJORDAN/JESSICARENE

eTicket number: **0167383790759**   Seats: **IAD-SFO** -
                                                                     SFO-IAD -

Purchase Summary

Method of payment: **Master Card ending in 2402**
Date of purchase: **Thu, Jul 25, 2019**

Airfare: 531.00 USD
U.S. Transportation Tax: 39.85 USD
U.S. Flight Segment Tax: 8.40 USD
September 11th Security Fee: 11.20 USD
U.S. Passenger Facility Charge: 9.00 USD

Total Per Passenger: **599.45 USD**

Total: **14386.80 USD**

Flight Information

Monday, August 26, 7:00 a.m.
United Airlines Flight 1181T
IAD > SFO
9:49 a.m. Arrival

Thursday, August 29, 9:30 a.m.
United Airlines Flight 516W
SFO > IAD
5:42 p.m. Arrival

Arrival in San Francisco

The group will meet at the United Airlines Domestic Baggage Claim where you will be greeted by two Stanford staff members and the shuttle drivers. You will be immediately transported to Stanford after everyone has arrived. If possible, please try to have carry-on luggage instead of checked bags to expedite time.

If you are not on the group flight but are arriving at SFO before, please let Russell Wald (rwald@stanford.edu) know if you plan on taking the shuttle to Stanford so we can ensure you have a seat.

If you plan on going directly to Stanford, please arrive no later than 11:00 a.m. and see the "Session Location" on this document for where we will meet.

Pre-reading

In advance of your arrival, reading and familiarizing yourself with the simulation documents is required. We will move quickly into sessions once you arrive and there will not be time to do an overview before the simulation.

In addition to the simulation reading you can access an optional primer on cybersecurity for those that would like greater context on the subject here.

Dress Style

The general attire is business casual. There will be a keynote dinner event on Tuesday evening, which is we recommend you wear business/dinner attire. There will also be a group photo at

this time. Below is a previous boot camp group photo for reference. Finally, while it is fairly warm at Stanford, the nights can be chilly. It is recommended that you bring a light sweater or coat with you.

Housing

You are staying at the Schwab Residential Center in the Stanford Graduate School of Business. You can check in your luggage at the end of the first night on Monday. Most events are on campus and within a short walking distance to the residences.

Session Location

The primary location of sessions and opening part of the boot camp will be at the Lou Henry Hoover Building Room 105, Annenberg Conference Room, 434 Galvez Mall, Stanford CA 94305.

Alcohol

The Ethics Committees do not allow for us to provide complimentary alcohol. There will be a few opportunities to enjoy a drink during the last two evening events. To avoid conflict, we have presumed a set price of $25 per day. We do not monitor this and it is on the honor system. It is suggested you make a check out to Stanford University if you do choose to partake in any consumption of the open alcohol that is made available.

Laptops

There will be a Hack Lab session and laptops are needed. Both Mac and PC will work.

Mobile Contact

Russell Wald, Senior Manager, External Affairs
(650) 850-9034

Trevor Carlsen, Manager, External Affairs
(707) 291-7595

Danielle Jablanksi, Manager, Cyber Programs
(563) 506-2817

First Name	Last Name	Job Title	Current Office or Committee	Chamber
Tristan	Abbey	Senior Professional Staff	Energy & Natural Resources Committee	Senate
Wendy	Anderson	Chief of Staff	Rep Val Demings	House
Karolina	Arias	Policy Advisor and Minority Staff Director	Senator Van Hollen Subcommittee on Securities, Investment, and Insurance	Senate
Virgilio	Barrera	Legislative Director	Senator Martin Heinrich	Senate
Charles	Carithers	Professional Staff Member	Committee on Homeland Security	House
Laura	Fullerton	Deputy Staff Director	House Foreign Affairs	House
Jessica	Hagens-Jordi	Defense and Foreign Policy Advisor	Rep. Jim Himes (HPSCI)	House
Katherine	Harris	Counsel for the Minority	Senate Select Committee on Intelligence	Senate
John Micah	Heinemann	Counsel	Financial Services Committee, Oversight and Investigations Subcommittee	House
Sunmin	Kim	Technology Policy Advisor	Sen. Schatz	Senate
Jacqueline	Maffucci	Policy Advisor	Homeland Security and Government Affairs Committee	Senate
Svetlana	Matt	Legislative Assistant	Office of Rep. Jerry McNerney (CA-09)	House
Sarah	Moxley	Staff Director	Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Innov	House
Jacob	Olidort	Foreign Policy Advisor	Office of Senator Josh Hawley	Senate
Cherilyn	Pascoe	Senior Professional Staff Member	Senate Commerce Committee	Senate
William	Payne	Chief Counsel	Sen. Ben Sasse/Senate Judiciary Committee	Senate
Asad	Ramzanali	Senior Advisor, Technology Policy	Office of Rep. Eshoo	House
John	Riordan	Professional Staff Member; Strategic forc	Senate Armed Services Committee	Senate
Michael	Seeds	Deputy Chief of Staff & Legislative Director	Rep. Mac Thornberry	House
Alicia	Smith	Counsel	Committee on Homeland Security	House
Stephen	Smith	Senior Policy Advisor	Senator Angus King	Senate
Katherine	Tai	Chief Trade Counsel, Trade Subcommittee	Ways and Means	House
Clinton	Trocchio	Deputy Clerk and Head of Analytics	Committee on Appropriations	Senate
Matthew	Williams	National Security Advisor	Sen. Kamala Harris	Senate
Robert	Winkler	Professional Staff Member	Senate Armed Services Committee	Senate

Cyber and Artificial Intelligence Boot Camp
August 26-29, 2019

The Hoover Institution, Annenberg Conference Room 105, Lou Henry Hoover Building
434 Galvez Mall, Stanford, CA 94305

LEADERSHIP

Andrew Grotto

Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI)

William J. Perry International Security Fellow, FSI

Research Fellow, Hoover Institution

Dr. Herb Lin

Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)

Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution

Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

CONTACTS

Danielle Jablanski, djablanski@stanford.edu +1(650) 725-4839

Cyber Program Manager, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute

Russell Wald, rwald@stanford.edu +1(202) 760-3204

Senior Manager for External Affairs

Hoover Institution, Stanford University

COURSE DESCRIPTION

Threats in cyberspace, innovations in emerging technology, complex digital interdependence and challenges for security, governance, privacy and safety capture headlines across the globe. Nations, companies and individuals are increasingly dependent on information and information technology for societal functions. Ensuring the security of. information and information technology — defined as cybersecurity — against a broad spectrum of hackers, criminals, terrorists, propagandists and state actors is a critical task for the nation. Challenges are evolving rapidly, with threats facing the nation and its infrastructure changing by the day.

Cybersecurity is not solely a technical matter, although it is easy for policy·analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, international relations, and a host of other disciplines. This Boot Camp draws upon the expertise of cyber and artificial intelligence scholars in academia as well as senior business leaders and security professionals in Silicon Valley and beyond, to provide perspectives on the many dimensions of this dynamic set of issues.

Artificial intelligence developments and are likewise being documented all over the world, with advances for medicine, automation, mobile apps, IoT devices, robotics, .and more. In collaboration with the Stanford Institute for Human-Centered Artificial Intelligence (HAI) recently launched at Stanford, the Boot Camp will introduce fundamentals of machine learning and AI. As the HAI mission states, the development of artificial intelligence should be paired with an ongoing study of its impact on human society and guided accordingly.

The 2019 Cyber and Artificial Intelligence Boot Camp for Congressional Staffers will incorporate multiple viewpoints and interactive sessions to provide an understanding of the fundamentals of cybersecurity and artificial intelligence, the nature of international security challenges and threats, various approaches to addressing these threats, and the development and use of capabilities to advance national interests. The Boot Camp seeks to give Congressional Staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the converging technology and policy issues of tomorrow.

- Scope: The security implications and challenges of the nation's use of information technology. The course focuses specifically on topics relevant for international security and policymaking. We will not dive deep on technological security products or processes for protecting or attacking systems and networks.

- Framing Theme #1: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem requires understanding the perspectives of various actors, their·interests and incentives. Boot Camp sessions are

designed to allow staffers to better understand the perspectives of different stakeholders and key players, including users, attackers, researchers, industry experts, and corporate executives.

- Framing Theme #2: The non-technical dimensions of offensive and defensive cybersecurity (politics, organizational and cultural dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.

- Framing Theme #3: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.

- Framing Theme #4: The expected global and multisector impacts of artificial intelligence cannot be understated. AI experts will provide fundamental primers for how algorithms and autonomous systems are built, how incorporation of this technology will affect society, and frameworks for how governments and publics thinking about the uses and misuses of technology in this new reality will evolve.

DAY 1 (Monday, August 26): Cyber Offense and Defense

11:30 am – 12:00 pm INTRODUCTION AND PROGRAM OVERVIEW

<u>Faculty:</u>
- **Andrew Grotto,** *Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI); Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Lunch available in Annenberg Conference Room

12:00 pm – 12:30 pm LUNCH KEYNOTE & WELCOME

<u>Opening Remarks:</u>
- H.R. McMaster, *Fouad and Michelle Ajami Senior Fellow, Hoover Institution; Former assistant to the president for National Security Affairs; Retired Lieutenant General, U.S. Army*

12:30 pm – 1:30 pm THINKING LIKE AN ATTACKER

<u>Faculty:</u>
- **Dr. Greg Conti,** *Senior Security Strategist, IronNet Cybersecurity*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Andrew Grotto,** *Stanford University (Moderator)*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

<u>Assignment:</u> While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

<u>Learning Objectives:</u> Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

1:30 pm – 1:45 pm BREAK

1:45 – 3:00 pm KEYNOTE: CURRENT THREAT LANDSCAPE

- **Kevin Mandia,** *Chief Executive Officer, FireEye*
- **Sean Kanuck,** *Visiting Fellow, Hoover Institution; Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence*
- Dr. Herb Lin, *Stanford University (Moderator)*

Threat actors and their specific activity signatures, global hot spots and trends, are analyzed daily by various security agencies, governments, and organizations. This keynote will direct our attention to today's principal threat actors, providing a bird's eye view of the threat landscape, current trends and capabilities, future outlook of malicious cyber activity, and seeks to bust certain myths sometimes circulated or recounted incorrectly about cyber operations. Speakers will also provide first-hand examples of experiences tracking threats and bad actors, and share insights about working in this field.

3:00 pm – 3:15 pm BREAK

3:15 pm – 4:15 pm THREATS TO CYBERSECURITY

<u>Faculty:</u>
- **Carey Nachenberg,** *Chief Scientist, Chronicle; Adjunct Assistant Professor of Computer Science, UCLA*
- Dr. Tom Berson, *Visiting Scholar, Stanford CISAC; Advisory Board Member, Salesforce; Founder, Anagram Laboratories*
- Dr. Herb Lin, *Stanford University (Moderator)*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. This session examines various known techniques and vulnerabilities in information technology that allow them to happen, painting a picture of a well-known cybersecurity theme: offense dominance. This session will include forensic case studies that illuminate the spectrum of the attack surface, key challenges, and trends.

<u>Learning Objectives</u>: Security-relevant principles of information technology; types of compromises; inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

4:15 pm – 4:30 pm BREAK

Dinner available in Annenberg Conference Room

4:30 pm – 5:30 pm DINNER: OFFENSIVE DIMENSIONS OF CYBERSECURITY

<u>Faculty:</u>
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Jason Kichen,** *Security Consultant*
- **Andrew Grotto,** *Stanford University (Moderator)*

Offensive activities — including those conducted for espionage and attack purposes — serve a variety of national goals. This discussion will summarize the operational and strategic requirements, intelligence needs, organizational structure and policy considerations necessary for offensive cyber operations.

<u>Learning Objectives</u>: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture, signaling, and other purposes; the differences between penetration and exploitation and their important distinctions; the scope and nature of U.S. command and control of offensive operations in cyberspace.

5:30 pm – 6:00 pm BREAK

Walk to Stanford Graduate School of Business, meet in room G101, Dunlevie Classroom

---

6:00 pm – 8:30 pm HOSPITAL RANSOMWARE SIMULATION (staffers only)

The hospital has been the victim of a cyber-attack in the form of ransomware which successfully encrypts 250,000 files and holds at least one system hostage, demanding a ransom payment in Bitcoin (BTC) in return for a decryption key which will unlock the system and restore access and functionality to the files. The hospital has a timeline of 72 hours to pay the ransom before their files become permanently encrypted and inaccessible, or are moved off their network.

Subject matter experts will act as executive leadership during the simulation, and staffers will be divided into teams to assist with directing action items, press releases, and critical decisions on how to manage the attack and response. Each team will have a coach aiding their organization and strategy. All names and information will be fictional, however, the simulated attack is based on previous real life scenarios. The information made available to participants is subject to change throughout the simulation. At the end of the exercise, teams will present their decision making processes to the hospital's CEO and Board of Trustees, and debrief on what it is like to face this type of cyber scenario in the real world. (Please see simulation packet for team information, simulation timeline, and background reading materials)

<u>Subject Matter Experts:</u>

Hospital Leadership:
> **Chief Executive Officer: Jamie Barnett,** Chief Marketing Officer, AppZen
> **Chief Strategy Officer: Amy Zhang,** Security Architect, Stanford Health Care

Information Technology Operations & Engineering Team
> **Tom Berson,** Visiting Scholar, Stanford CISAC; Advisory Board Member, Salesforce; Founder, Anagram Laboratories

Cybersecurity & Access Management Team
> **John Maguire,** The Chertoff Group, Former Senate Select Committee on Intelligence Staff, U.S. Navy

Public Relations & Communications Team
> **Subject Matter Expert: Victoria Tung,** Director, Government and Public Affairs, Texas Instruments

Legal & Risk Management Team
> **Subject Matter Expert: Beth George,** Affiliate, CISAC, Partner, Wilson Sonsini Goodrich & Rosati

Privacy & Compliance Team
> **Subject Matter Expert: Ruby Zefo,** Chief Privacy Officer, Uber

Additional Volunteers:
> **Jared Sperli,** Senior Manager, IT Security, Stanford Health Care

DAY 2 (Tuesday, August 27): Technical & Nontechnical Approaches

---

8:30 am – 9:00 am BREAKFAST AND DAY 1 DEBRIEF

- **Andrew Grotto**, *Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI); Research Fellow, Hoover Institution*
- **Dr. Herb Lin**, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:00 am – 11:00 am HANDS ON HACK LAB

<u>Faculty:</u>
- **Alex Stamos**, *Director, Internet Observatory, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI); Visiting Fellow, Hoover Institution; Adjunct Professor, Stanford University*

Stamos' course provides an introduction to the most common types of attacks used in cybercrime and cyberwarfare. As a long-time security practitioner, he covers the basics of an area of technology and how it has been misused. Participants will complete a lab session from his Stanford course in which they will be guided through attacking a known insecure system using techniques and tools seen in the field.

Participants will be required to bring a Windows or Mac laptop and will be provided with basic information for the exercise prior to the session. No computer science background is necessary for this session.

11:00 am – 11:15 am BREAK

Lunch available in Annenberg Conference Room

11:15 am – 12:15 pm LUNCH: CYBER RISK, ECONOMICS, AND ORGANIZATIONAL DIMENSIONS OF CYBERSPACE

Faculty:
- **Dr. Tyler Moore,** *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*
- **Dr. Greg Falco,** *Research Scholar, Stanford CISAC*
- Dr. Herb Lin, *Stanford University (Moderator)*

Known cybersecurity measures are often not fully adopted due to a variety of economic and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. The insurance sector is working to provide accurate and adequate coverage for this market. This session examines how these factors often discourage the adoption of sound security practices.

Learning Objectives: The importance of economic and organizational factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

12:15 pm – 12:30 pm BREAK

12:30 pm – 1:30 pm PRIVACY & SECURITY FOR CONSUMERS, CUSTOMERS, AND CRITICAL INFRASTRUCTURE

Faculty:
- **Robert Chesney,** *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*
- **Dr. Jennifer King,** *Director of Consumer Privacy, Center for Internet and Society, Stanford Law School*
- **Ted Gizewski,** *Vice President, Product Legal, Salesforce*
- **Andrew Grotto,** *Stanford University (Moderator)*

Privacy and security risks manifest differently in different business sectors. They also share important interdependencies that require integrated risk management and policy-making strategies.

Learning objectives: Gaining insight into how privacy and security risks affect different sectors, how risk management strategies must be tailored to the risk environment, and why an integrated approach to managing privacy and security risks is imperative.

1:30 pm – 1:45 pm BREAK

1:45 pm – 2:45 pm INTERNATIONAL LAW AND CYBERSECURITY

Faculty:
- **Dr. Tess Bridgeman,** *Affiliate, CISAC; Senior Fellow, Center on Law and Security, NYU*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Andrew Grotto,** *Stanford University (Moderator)*

Nations have increasingly engaged in cyber influence operations and other types of cyber activity – ranging from cyber espionage to cyber-attacks with physical world consequences – to advance their national interests and gain competitive advantage in their international relations. At the same time, there have been some successful and some stalled efforts to achieve consensus among nations on the norms governing responsible state behavior in cyberspace. An understanding of the international law governing cyber activity by states and, in particular, those that operate with respect to cyber activity that falls below the threshold of a use of force or "armed attack," is imperative to assessing policy options and responding to foreign states' cyber operations.

Learning Objectives: How to apply international law to cyber activity conducted by states and their proxies, including cyber influence operations and uses of force in cyberspace; understand the legal and policy tools available to states to address adversarial cyber operations.

2:45 pm – 3:45 pm FUNDAMENTALS OF DEFENSE FOR CYBERSECURITY

Faculty:
- **Dr. Irving Lachow,** *Visiting Fellow, Hoover Institution; Affiliate, CISAC; Deputy Director, Cyber Strategy and Execution, MITRE*
- **Andrew Grotto,** *Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI); Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Cybersecurity can be a deeply technical subject, especially when it comes to how cybersecurity solutions are implemented. A few fundamental principles underlie most solutions. This session takes a deep dive into the principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity, understanding interdependencies, and how to use fundamentals and understanding collectively to improve security.

3:45 pm – 4:00 pm BREAK

4:00 pm – 5:00 pm CYBER ENABLED INFORMATION WARFARE AND INFLUENCE OPERATIONS

Faculty:
- **Dr. Rosanna Guadagno,** *Director, Information Warfare Working Group, Stanford University*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Andrew Grotto,** *Stanford University (Moderator)*

Cyber-enabled information warfare is fundamentally different than cyber war and cyber conflict, at least as the latter are generally understood today in the policy world. Cyber war and cyber conflict target information and information technology systems, whereas cyber-enabled information warfare targets human minds. Russia did not "hack" Facebook, YouTube and Twitter by penetrating their security—it used those platforms exactly as they were designed to be used. This session delves into these differences, placing the emphasis on the psychological vulnerabilities of people that the Russians (and other institutional users of social media) exploit for gain.

Learning Objectives: Understanding the fundamental differences between cyber war and cyber-enabled information warfare; the psychology underlying cyber-enabled information warfare; and the present inadequacies of the U.S. government in coping with such warfare.

5:00 pm BREAK

Please make your way to Blount Hall at the David and Joan Traitel Building for dinner

6:30 pm – 9:00 pm KEYNOTE RECEPTION & DINNER: PERSPECTIVES ON GOVERNANCE OF ARTIFICIAL INTELLIGENCE

- Dr. John Etchemendy, *Co-Director, Stanford Institute for Human-Centered Artificial Intelligence; Provost Emeritus, and Patrick Suppes Family Professor in the School of Humanities, Stanford University*
- Reid Hoffman, *Partner, Greylock Partners; Co-founder and former Executive Chairman, LinkedIn*
- **Ambassador Michael McFaul,** *Senior Fellow, Freeman Spogli Institute for International Studies (FSI); Senior Fellow, Hoover Institution, Stanford University (Moderator)*

Artificial intelligence technologies are augmenting human capability and efficiency, changing the way we think about and interact with information, and creating new governance challenges and opportunities for policy makers and business leaders. Please join two distinguished thought leaders to discuss critical issues facing the future of human-centered AI development, innovation, and governance.

DAY 3 (Wednesday, August 28): Industry Voices, and the Future of Artificial Intelligence

---

9:00 am – 9:30 am BREAKFAST AND DAY 2 DEBRIEF

- **Andrew Grotto,** *Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute (FSI); Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:30 am – 10:45 am INDUSTRY PERSPECTIVES PANEL (Off-the-Record)

<u>Faculty:</u>
- **Raj Shah (Chair),** *Visiting Fellow, Hoover Institution; Co-CEO, Arceo.ai*
- **Frank Chen,** *Partner, Andreessen Horowitz*
- **Michelle Finneran Dennedy,** *Chief Executive Officer, DrumWave Inc.*
- **Rick Howard,** *Chief Security Officer, Palo Alto Networks*
- **Dr. Mark Rosekind,** *Chief Safety Innovation Officer, Zoox*

Market forces have a critical role in enhancing or weakening security and privacy considerations. This session examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "ground truths" about the security problems facing the private sector.

<u>Learning Objectives</u>: Various private sector perspectives on technology and relations beyond Silicon Valley from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity and AI.

10:45 am – 11:00 am BREAK

11:00 am – 12:00 pm FUNDAMENTALS OF AI AND MACHINE LEARNING

<u>Faculty:</u>
- Dr. Emma Brunskill, *Assistant Professor, Computer Science, Stanford University; Stanford AI for Human Impact Lab*
- **Dr. Jeff Clune,** *Harris Associate Professor, Computer Science, University of Wyoming*
- Andrew Grotto, *Stanford University, (Moderator)*

There have been massive advances in artificial intelligence, machine learning, and robotics, especially those fueled by deep neural networks (aka deep learning, including deep reinforcement learning). These technologies are currently being heavily invested in and deployed by companies, organizations, and militaries around the world. They will likely substantially affect nearly every sector of society and the world economy, and in some cases entirely disrupt them. This session will explain the basic elements of artificial intelligence, with a focus on deep neural networks. It will also discuss the application areas they have already excelled in as well as some worrisome use cases that policy makers should be aware of.

Learning Objectives: A general understanding of machine learning, deep neural networks, and deep reinforcement learning. An overview of the practical applications and limits of these technologies, as well as current and future use cases (both positive and negative).

12:15 pm – 1:15 pm KEYNOTE LUNCH: ARTIFICIAL INTELLIGENCE AND SAFETY

- Dr. Fei-Fei Li, *Co-Director, Stanford Institute for Human-Centered Artificial Intelligence, Stanford University; Professor, Computer Science, Stanford University*
- Dr. Mykel Kochenderfer, *Assistant Professor of Aeronautics and Astronautics, Stanford University; Director, Stanford Intelligent Systems Laboratory*
- **Andrew Grotto**, *Stanford University (Moderator)*

Building robust decision making systems is challenging, especially for safety critical systems such as unmanned aircraft and driverless cars. Decisions must be made based on imperfect information about the environment and with uncertainty about how the environment will evolve. In addition, these systems must carefully balance safety with other considerations, such as operational efficiency. Typically, the space of edge cases is vast, placing a large burden on human designers to anticipate problem scenarios and develop ways to resolve them.

Learning Objectives: We will discuss ways in which artificial intelligence can be applied to the design of these safety critical systems. This approach has the potential to significantly improve robustness of these systems, but there are two major challenges. The first is in ensuring computational tractability, and the other is establishing trust in their correct operation when deployed in the real world. We will outline some methodologies for addressing these challenges.

1:15 pm – 1:30 pm BREAK

Faculty:
- Dr. John Villasenor, *Visiting Fellow, Hoover Institution; Professor of Electrical Engineering, Law, Public Policy, and Management, University of California Los Angeles*
- Dr. Patrick Lin, *Director, Emerging Sciences Group, California Polytechnic State University*
- Dr. Herb Lin, *Stanford University (Moderator)*

Advances in AI are raising a set of fundamentally important questions that go well beyond technology. This session will explore key AI ethics and governance issues, such as the nuances and challenges of addressing questions like: What should the rules be when machines make decisions with ethical implications, and who writes those rules? How can the issue of bias in AI be addressed?

Learning Objectives: The sorts of governance structures that can best ensure a climate of innovation in the AI ecosystem while also protecting against its potential misuses. What special issues are raised by AI in defense and security specifically.

Walk to Hoover Tower

2:40 pm – 3:50 pm HOOVER TOWER AND ARCHIVES TOUR (Staffers only)

Faculty:
- Jean Cannon, *Curator, North American Collections, Hoover Institution Library & Archives*

Founded by Herbert Hoover in 1919, the Hoover Institution Library & Archives are dedicated to documenting war, revolution, and peace in the twentieth and twenty-first centuries. With nearly one million volumes and more than six thousand archival collections from 171 countries, Hoover supports a vibrant community of scholars and a broad public interest in the meaning and role of history.

Travel to Center for Automotive Research at Stanford
SHUTTLE ARRIVES AT 3:50PM TO END OF GALVEZ ST.

> **4:15 pm – 5:30 pm VISIT TO CENTER FOR AUTOMOTIVE RESEARCH AT STANFORD**
> (Staffers only)

<u>Faculty:</u>
- Dr. Stephen Zoepf, *Executive Director, Center for Automotive Research, Stanford University*
- Bryan Casey, *Lecturer in Law, Stanford University*
- Dr. Marco Pavone, *Associate Professor, Aeronautics and Astronautics, Stanford University*

The Center for Automotive Research at Stanford (CARS) brings together researchers, students, industry, government and the community to enable a future of human-centered mobility. Understanding how people and machines work together has never been so important than when building vehicles of the future. CARS supports educational experiences for students, infrastructure for research and events that bring students and campus researchers together with industry professionals and the broader community. Researchers and vehicles affiliated with CARS are housed at the Automotive Innovation Facility, which houses the Volkswagen Automotive Innovation Lab (often referred to as 'VAIL'), a state-of-the-art vehicle research facility where interdisciplinary teams can work on projects that move vehicle human-centered mobility forward.

Participants will visit CARS' Automotive Innovation Facility and hear from researchers on the cutting edge of the development of autonomous vehicles. Experts will brief the group on trends in the field, ongoing legal and ethical debates, and provide a tour of the facility showcasing vehicles and a driving simulator used for research.

Ride to Stanford Golf Course - SHUTTLE ARRIVES AT 5:45PM AT CARS*

> **6:00 pm – 8:00 pm DINNER AND REFLECTIONS (Staffers only)**

Coupa Café – Stanford
198 Junipero Serra Blvd, Stanford, CA, 94305

Ride to Schwab Residential Hall - SHUTTLE ARRIVES AT 8:15pm*

Thursday, August 29: Shuttle will arrive to Schwab Residential Hall at 6:30am to depart for San Francisco International Airport